# On fields with the Property (B)

Francesco Amoroso, Sinnou David, Umberto Zannier

# On fields with the Property (B)

Francesco Amoroso, Sinnou David and Umberto Zannier

*Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139*
*Université de Caen, Campus II, BP 5186*
*14032 Caen Cedex, France*

*Institut de Mathématiques, CNRS UMR 7586*
*Université Pierre et Marie Curie, 4, place Jussieu*
*75252 Paris Cedex 05*

*Scuola Normale Superiore*
*Piazza dei Cavalieri, 7*
*56126 Pisa, Italia*

**Abstract.**
Let $K$ be a number field and let $L/K$ be an infinite Galois extension with Galois group $G$. Let us assume that $G/Z(G)$ has finite exponent. We show that $L$ has the Property (B) of Bombieri and Zannier: the absolute and logarithmic Weil height on $L^*$ (outside the set of roots of unity) is bounded from below by an absolute constant. We discuss some feature of Property (B): stability by algebraic extensions, relations with field arithmetic. As a as a side result, we prove that the Galois group over $\mathbb{Q}$ of the compositum of all totally real fields is torsion free.

**Mathematics Subject Classification:** 11G5O (Primary), 12E30 (Secondary).

## 1 Introduction

Let $h$ be the absolute and logarithmic Weil height on $\overline{\mathbb{Q}}$. Following Bombieri and Zannieri [Bo-Za], we say that a set $\mathcal{A}$ of algebraic numbers has the *Bogomolov property* (B) if there exists a real number $T_0 = T_0(\mathcal{A}) > 0$ such that the set of non-zero $\alpha \in \mathcal{A}$ of height $< T_0$ consists of all roots of unity in $\mathcal{A}$.

There are several interesting examples of subfields of $\overline{\mathbb{Q}}$ with Property (B). For instance, the field $\mathbb{Q}^{tr}$ of all totally real algebraic numbers has this property (see [Sc] and [Sm]). Also the abelian closure $\mathbb{Q}^{ab}$ satisfies (B) (see [Am-Dv]) and, more generally, the abelian closure $K^{\mathrm{ab}}$ of a number field $K$ satisfies (B) (see [Am-Za]). In the latter case, Property (B) holds uniformly in $[K : \mathbb{Q}]$; the height on $(K^{\mathrm{ab}})^*$ outside roots of unity is bounded from below by a positive constant depending only on $[K : \mathbb{Q}]$ (see [Am-Za2]).

Another family of fields with Property (B) is provided by fields with bounded local degrees at some finite place. Let $K$ be a number field and $L/K$ be an infinite extension.

Fix a non-archimedean valuation $v$ of $K$. We say that $L/K$ has bounded local degree at $v$ if there exists an integer $d_0$ such that for every extension $w$ of $v$ to $L$ we have $[L_w : K_v] \leq d_0$. Bombieri and Zannier prove (see [Bo-Za], Theorem 2) that a Galois extension $L/\mathbb{Q}$ with bounded local degree at some rational prime satisfies the Property (B).

A third family has been recently exhibited by Habegger [Hab]. Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then the field $\mathbb{Q}(E_{\mathrm{tors}})$ obtained by adjoining all torsion points of $E$ has the Bogomolov property. Observe that if $E$ does not have complex multiplication then this field is an infinite non-abelian extension of $\mathbb{Q}$.

The first two examples above suggest the following problem.

**Problem 1.1** *Let $K/\mathbb{Q}$ be an extension with bounded local degree at some rational prime. Is it true that $K^{\mathrm{ab}}$ has the Property (B)?*

The first result of this article is a partial answer to this problem. In section 4 we prove the following generalization of both [Bo-Za], Theorem 2 and [Am-Za2], Theorem 1.2.

**Theorem 1.2** *Let $K$ be a number field and let $L/K$ be an infinite Galois extension with Galois group $G$. Let $E \subseteq L$ be the subfield fixed by $Z(G)$ and assume that $E/K$ has local degree at some non-archimedean valuation $v$ of $K$ bounded by $d_0$. Then $L$ has the Property (B), uniformly in $v$, $d_0$ and $[K : \mathbb{Q}]$.*

*More explicitely, there exists a positive function $c$ which depends effectively only on $v$, $d_0$ and $[K : \mathbb{Q}]$ such that for any $\alpha \in L^*$ which is not a root of unity we have $h(\alpha) \geq c$.*

As a special case of the quoted result of Bombieri and Zannier, a Galois extension $L/\mathbb{Q}$ with Galois group of finite exponent has Property (B). Indeed $\mathrm{Gal}(L/K)$ has finite exponent if and only if $L/K$ has uniformly bounded local degrees at every prime of $K$ (see [Ch], Theorem 2.2.2, for a more precise statement). Similarly, our Theorem 1.2 implies:

**Corollary 1.3** *Let $K$ be a number field and let $L/K$ be an infinite Galois extension with Galois group $G$. Let us assume that $G/Z(G)$ has finite exponent $b$. Then $L$ has the Property (B), uniformly in $b$ and $[K : \mathbb{Q}]$.*

Our second result deals with finite extensions $F/L$ of a field $L$ with Property (B). Assume that $L/K$ is an abelian extension of a number field $K$. By the main theorem of [Am-Za], $F$ has the Property (B). Similarly, if $L/\mathbb{Q}$ has bounded local degree at some rational prime, then $F/\mathbb{Q}$ has the same property and thus, by [Bo-Za], it has the Property (B). Therefore the following question arises naturally.

**Problem 1.4** *Let $L$ be a field with Property (B) and let $F/L$ be a finite extension. Is it true that $F$ has necessarily Property (B)?*

In section 5 we give a negative answer to this question and we provide some related remarks.

In this respect, it may not be out of place to recall another definition of [Bo-Za] (see also [Dv-Za]). A set $\mathcal{A}$ of algebraic numbers has the *Northcott property* (N) if there exists a positive real number $T$ such that the set of $\alpha \in \mathcal{A}$ of height $< T$ is finite. By a celebrated theorem of Northcott, the set of algebraic numbers of degree at most $d$ has Property (N). Moreover, it is easy to see that if an extension $L/\mathbb{Q}$ has Property (N), then every finite

extension $F/L$ has again (N). Thus Property (B) and Property (N) behave in radically different ways under finite extensions.

Section 6 explores some speculative relations between Property (B) and field arithmetic. Two central definitions in this area are Pseudo Algebraically Closed and Hilbertian fields. We recall that a field $K$ is Pseudo Algebraically Closed (PAC) if each absolutely irreducible variety defined over $K$ has a $K$-rational point (see [Fr-Ja], chapter 11, for more details). A field $K$ is Hilbertian if it satisfies Hilbert's Irreduciblity Theorem: for every irreducible $f \in K[x,y]$ which is separable in $x$ there exists $a \in K$ such that $f(x,a)$ is irreducible over $K$ (see [Fr-Ja], chapter 12, for more details).

We consider the following problems. Does there exist a PAC field $K \subseteq \overline{\mathbb{Q}}$ which satisfies (B)? What are the relations between (B) and hilbertianity ?

We give some evidence for a negative answer to the first question and we provide examples of a Hilbertian (resp. non Hilbertian) field which does not satisfy (resp. which satisfies) Property (B).

Finally, in section 7 we prove that the Galois group over $\mathbb{Q}$ of the compositum of all totally real fields is torsion free. This results is needed in section 5, and it is apparently not known.

**Aknowledgements.** The authors are indebted with P. Dèbes, B. Deschamps and M. Fried for useful discussions on the subject of sections 6 and 7. We also thank D. Simon who provides us with the reference [Ko].

## 2 Notations and auxiliary results

Let $K$ be a number field. Given a place $v$ of $K$ we denote by $|\cdot|_v$ the corresponding absolute value normalized so to induce on $\mathbb{Q}$ one of the standard absolute values.

We shall use the followings couple of lemmas.

**Lemma 2.1** *Let $K$ be a number field, $v$ be a finite place of $K$ over a rational prime $p$ and let $\rho > 0$. Let $\gamma_1$, $\gamma_2 \in \mathcal{O}_K$ such that $|\gamma_1 - \gamma_2|_v \leq p^{-\rho}$. Then for any non-negative integer $\lambda$ we have $|\gamma_1^{p^\lambda} - \gamma_2^{p^\lambda}|_v \leq p^{-s(p,\rho,\lambda)}$ with $s(p,\rho,\lambda) \to +\infty$ for $\lambda \to +\infty$.*

*More precisely, let us define an integer $k = k(p,\rho)$ by $k = 0$ if $(p-1)\rho > 1$ and by*

$$p^{k-1}(p-1)\rho \leq 1 < p^k(p-1)\rho$$

*otherwise. Then*

$$s(p,\rho,\lambda) = p^k\rho + \max(0, \lambda - k) \ .$$

**Proof.** Let us denote by the same letter $v$ the only valuation of $K(\zeta_{p^\lambda})$ extending $v$. We write

$$\gamma_1^{p^\lambda} - \gamma_2^{p^\lambda} = (\gamma_1 - \gamma_2) \prod_{j=1}^{\lambda} \prod_{\zeta_{p^j}} (\gamma_1 - \zeta_{p^j}\gamma_2)$$

where the inner product is on the roots of unity $\zeta_{p^j}$ of order $p^j$. The ultrametric inequality shows that

$$|\gamma_1 - \zeta_{p^j}\gamma_2|_v = |\gamma_1 - \gamma_2 + (1 - \zeta_{p^j})\gamma_2|_v \leq \max(p^{-\rho}, p^{-1/p^{j-1}(p-1)}) \ .$$

Then $|\gamma_1^{p^\lambda} - \gamma_2^{p^\lambda}|_v \leq p^{-s}$ with

$$s = \rho + \sum_{j=1}^{\lambda} \min(p^{j-1}(p-1)\rho, 1) = p^k\rho + \max(0, \lambda - k) \; .$$

□

**Lemma 2.2** *Let $L/K$ be a Galois extension of number fields and let $\sigma \in \mathrm{Gal}(L/K)$. Let $\wp$ be a prime of $\mathcal{O}_K$ over the rational prime $p$. Let also $a$, $b \in \mathbb{N}$ and $\rho > 0$. Let us assume that*

$$\forall \gamma \in \mathcal{O}_L, \quad \forall v \,|\, \wp, \qquad |\gamma^a - \sigma(\gamma)^b|_v \leq p^{-\rho} \; .$$

*Then for every $\alpha \in L$ such that $\alpha^a \neq \sigma(\alpha)^b$ we have*

$$h(\alpha) \geq \frac{1}{a+b}\left(\frac{[K_\wp : \mathbb{Q}_p]}{[K:\mathbb{Q}]}\rho \log p - \log 2\right); .$$

**Proof.**

We have already used implicitly this lemma in the proofs of [Am-Dv], Proposition 1, and of [Am-Za2], Proposition 3.2. We briefly recall the demonstration.

Let $v$ be a place of $L$, normalized so to induce on $\mathbb{Q}$ one of the standard places. We shall estimate $|\alpha^a - \sigma(\alpha)^b|_v$. Suppose to start with that $v|\wp$.

By the Strong Approximation Theorem, there exists an integer $\beta \in L$ such that $\alpha\beta$ is integer and

$$|\beta|_v = \max\{1, |\alpha|_v\}^{-1}.$$

(see [Am-Dv], lemma 1, for details). Then we have $|(\alpha\beta)^a - \sigma(\alpha\beta)^b|_v \leq p^{-\rho}$ and $|\beta^a - \sigma(\beta)^b|_v \leq p^{-\rho}$. Using the ultrametric inequality, we deduce that

$$|\alpha^a - \sigma(\alpha)^b|_v = |\beta|_v^{-a}|(\alpha\beta)^a - \sigma(\alpha\beta)^b + (\sigma(\beta)^b - \beta^a)\sigma(\alpha)^b|_v$$

$$\leq c(v)\max(1, |\alpha|_v)^a \max(1, |\sigma(\alpha)|_v)^b$$

with $c(v) = p^{-\rho}$. This last inequality plainly holds for an arbitrary place $v$ of $L$ with

$$c(v) = \begin{cases} 1 & \text{if } v \nmid \infty \; ; \\ 2 & \text{if } v \,|\, \infty \; . \end{cases}$$

Applying the Product Formula as in [Am-Za2], Proposition 3.2, to $\alpha^a - \sigma(\alpha)^b$ we get, after a standard computation,

$$1 \leq 2^{[K:\mathbb{Q}]} p^{\rho[K_\wp:\mathbb{Q}_p]} H(\alpha)^{a[K:\mathbb{Q}]} H(\sigma(\alpha))^{b[K:\mathbb{Q}]} \; .$$

The conclusion follows.

□

We now fix some notations which we follow in the next two sections.

Let $K$ be a number field of degree $d$ over $\mathbb{Q}$. We consider a finite Galois extension $L/K$ of Galois group $G$. Let $N$ be a normal subgroup of $G$ contained in $Z(G)$. We let $E = L^N$ be the fixed field of $N$. We remark that $N$ is abelian (since it is contained in $Z(G)$). Thus $L/E$ is an abelian extension of Galois group $N$.

We fix a prime ideal $\mathfrak{q}$ of $\mathcal{O}_E$. Let $\wp = \mathfrak{q} \cap \mathcal{O}_K$ and let $(p) = \wp \cap \mathbb{Z}$. We define $d_0$ as the local degree $[E_{\mathfrak{q}} : K_{\wp}]$.

We also denote by $\boldsymbol{\mu}$ the group of roots of unity and by $\boldsymbol{\mu}_{p^\infty}$ the group of roots of unity of order a $p$-th power.

# 3 A conditional result

The main result of this section is the following generalization of Proposition 3.2 of [Am-Za2].

**Proposition 3.1** *Let $\alpha \in L^* \backslash \boldsymbol{\mu}$. Assume further that for any $\tau \in \mathrm{Gal}(L/E)$*

$$\tau(\alpha)/\alpha \notin \boldsymbol{\mu}_{p^\infty} \backslash \{1\} \; . \tag{3.1}$$

*Then*

$$h(\alpha) \geq c$$

*for some $c > 0$ depending only on $p$, $d_0$ and $d$.*

**Proof.** We can assume $L = E(\alpha)$. Indeed $\mathrm{Gal}(E(\alpha)/E)$ is a normal subgroup of $\mathrm{Gal}(E(\alpha)/K)$ contained in the center. Thus, condition (3.1) can be rephrased by saying that for any non-trivial $\tau \in \mathrm{Gal}(L/E)$ we have $\tau(\alpha)/\alpha \notin \boldsymbol{\mu}_{p^\infty}$.

A first case occurs when $\mathfrak{q}$ does not ramify in $L$. Let $\phi$ be the Frobenius automorphism of $\mathfrak{Q}/\mathfrak{q}$, where $\mathfrak{Q}$ is any prime of $\mathcal{O}_L$ over $\mathfrak{q}$. Since $L/E$ is abelian, $\phi$ does not depend on the choice of $\mathfrak{Q}$. Thus for any $\gamma \in \mathcal{O}_L$

$$\gamma^q \equiv \phi(\gamma) \bmod \mathfrak{q}\mathcal{O}_L \; ,$$

where $q$ is the norm of $\mathfrak{q}$. Let now $\mathfrak{q}'$ be an other prime ideal of $\mathcal{O}_E$ over $\wp$, fix a prime $\mathfrak{Q}'$ of $\mathcal{O}_L$ over $\mathfrak{q}'$ and let $\phi'$ be the Frobenius of $\mathfrak{Q}'/\mathfrak{q}'$. Then $\phi$ and $\phi'$ are both in $N$ and are conjugate in $G$. Since $N$ is contained in $Z(G)$ we deduce that $\phi' = \phi$. This shows that for any $\gamma \in \mathcal{O}_L$ and for any place $v$ of $L$ with $v \,|\, \wp$ we have

$$|\gamma^q - \phi(\gamma)|_v \leq p^{-1/e_0} \; ,$$

where $e_0$ is the ramification index of $\mathfrak{q}$ over $\wp$.

Lemma 2.1 shows that there exists $\lambda$ depending only on $p$, on $e_0$ and on $d$ such that

$$|\gamma^{qp^\lambda} - \phi(\gamma)^{p^\lambda}|_v \leq p^{-2d} \; .$$

Since $\alpha$ is not a root of unity, $\alpha^{qp^\lambda} - \phi(\alpha)^{p^\lambda} \neq 0$. By lemma 2.2

$$h(\alpha) \geq \frac{1}{p^\lambda(q+1)}(2[K_\wp : \mathbb{Q}_p] \log p - \log 2) \geq \frac{\log 2}{p^\lambda(q+1)} \geq c_1$$

for some $c_1 > 0$ depending only on $p$, $d_0$ and $d$.

Assume now that $\wp$ is ramified in $L$ and let, as in [Am-Za2] Proposition 2.3,

$$H_{\mathfrak{q}} := \{\sigma \in N \text{ such that } \forall \gamma \in \mathcal{O}_L,\ \sigma\gamma^q \equiv \gamma^q \bmod \mathfrak{q}\mathcal{O}_L\}$$

where $q$ is the norm of $\mathfrak{q}$. By the quoted proposition, $H_{\mathfrak{q}}$ is non trivial. As in the non-ramified case, let $\mathfrak{q}'$ be an other prime ideal of $\mathcal{O}_E$ over $\wp$. Then $H_{\mathfrak{q}}$ and $H_{\mathfrak{q}'}$ are both subgroups of $N$ and are conjugate in $G$. Since $N$ is contained in $Z(G)$ we deduce that $H_{\mathfrak{q}'} = H_{\mathfrak{q}}$. Let $\sigma$ be a non trivial automorphism of this subgroup. Then, for any $\gamma \in \mathcal{O}_L$ and for any place $v$ of $L$ with $v \mid \wp$ we have

$$|\gamma^q - \sigma(\gamma)^q|_v \leq p^{-1/e_0}\ ,$$

where $e_0$ is the ramification index of $\mathfrak{q}$ over $\wp$. We use Lemma 2.1 and Lemma 2.2 as in the first part of the proof. We remark that $\alpha^{qp^\lambda} - \sigma(\alpha)^{qp^\lambda} \neq 0$ thanks to (3.1) and to the remark at the beginning of the proof. We get $h(\alpha) \geq c_2$ for some $c_2 > 0$ depending only on $p$, $d_0$ and $d$. It is now enough to choose $c = \min(c_1, c_2)$.

□

# 4 An unconditional result and the proof of Theorem 1.2

The radical reduction of [Am-Za2], section 4, does not apply in the present situation. Indeed, following the beginning of the proof of Proposition 4.3 in *op. cit.*, $k$ is not necessarily a power of a prime and so we cannot bound the degree of $E(\zeta_k)/E$ in terms of $d_0$ and $d$.

Fortunately, we can modify the argument of *op.cit.* in a such a way that it applies in the present situation. As an extra-bonus the proof becomes simpler.

We first state a simplified and slightly precise version of a special case of [Am-Za2], Lemma 4.2. The present statement applies only to subgroups of $(\mathbb{Z}/k\mathbb{Z})^*$ for $k$ a prime power, but this is enough for our purposes.

**Lemma 4.1** *Let $p$ be a rational prime, $k$ be a $p$-th power and $B$ be a positive integer. Then, for every subgroup $H$ of $(\mathbb{Z}/k\mathbb{Z})^*$ of index $< B$, there are integers $x$, $y$ such that $x \bmod k \in H$, $y \bmod k \in H$ and*

$$2 < y - x < 6B\ .$$

**Proof.** The proof is a standard application of the box principle. Let $\Lambda = \{x \in \mathbb{N} \mid x \bmod k \in H\}$ and define, for $j \in \mathbb{N}$, the real interval

$$I_j = [6(j-1)B, 6jB)\ .$$

Assume by contradiction

$$\forall j \in \mathbb{N}, \qquad |I_j \cap \Lambda| \leq 3\ .$$

Let $J$ be a large integer and put $r = [6JB/k]$. Then

$$r|H| = |\Lambda \cap [0, rk)| \leq |\Lambda \cap [0, 6JB)| \leq 3J$$

which implies $2B|H| \leq 6JB/r \leq k(r+1)/r$. Letting $J \to +\infty$ we get a contradiction:

$$2B|H| \leq k \leq 2(1-1/p)k = 2|(\mathbb{Z}/k\mathbb{Z})^*| < 2B|H|\ .$$

Thus there exist integers $x = x_1 < x_2 < x_3 < x_4 = y$ such that $x_i \bmod k \in H$ and $y - x < 6B$.

□

We can now prove an unconditional version of Proposition 3.1.

**Proposition 4.2** *Let $\alpha \in L^* \backslash \boldsymbol{\mu}$. Then*

$$h(\alpha) \geq c'$$

*for some $c' > 0$ depending only on $p$, $d_0$ and $d$.*

**Proof.** There exists a $p$-th power $k$ and a primitive $k$-root of unity $\zeta_k \in L$ such that

$$L \cap \mathbb{Q}(\boldsymbol{\mu}_{p^\infty}) = L \cap \mathbb{Q}(\zeta_k) \; .$$

We identify $\mathrm{Gal}(E(\zeta_k)/E)$ to a subgroup of $(\mathbb{Z}/k\mathbb{Z})^*$ of index, say, $B-1$. By Galois theory, $B - 1 = [E \cap \mathbb{Q}(\zeta_k) : \mathbb{Q}]$. Since $k$ is a $p$-th power, the prime $p$ is totally ramified in $E \cap \mathbb{Q}(\zeta_k)$. This shows that $B - 1 \leq e(\mathfrak{q}|p) \leq d_0 d$. By Lemma 4.1 there exist $\sigma_1$, $\sigma_2 \in \mathrm{Gal}(E(\zeta_k)/E)$ such that $\sigma_i \zeta_k = \zeta_k^{g_i}$ with $g = g_2 - g_1$ satisfiying

$$2 < g < 6(d_0 d + 1) \; . \tag{4.1}$$

Let $\tilde{\sigma}_i \in \mathrm{Gal}(L/E)$ extending $\sigma_i$. We want to apply Proposition 3.1 with $\alpha \leftarrow \beta$, where

$$\beta = \frac{\tilde{\sigma}_2(\alpha)}{\alpha^g \tilde{\sigma}_1(\alpha)} \; . \tag{4.2}$$

To do this we need to prove that $\beta \notin \boldsymbol{\mu}$ and that $\tau(\beta)/\beta \notin \boldsymbol{\mu}_{p^\infty} \backslash \{1\}$ for any $\tau \in \mathrm{Gal}(L/E)$. Let us verify these requirements. We argue by contradiction.

- $\beta \in \boldsymbol{\mu}$.

Then, by (4.2),

$$gh(\alpha) = h(\alpha^g) = h(\tilde{\sigma}_2(\alpha)/\tilde{\sigma}_1(\alpha)) \leq 2h(\alpha) \; .$$

Since $g > 2$ by (4.1) we get $\alpha \in \boldsymbol{\mu}$. Contradiction.

- There exists $\tau \in \mathrm{Gal}(L/E)$ such that $\theta := \tau(\beta)/\beta \in \boldsymbol{\mu}_{p^\infty} \backslash \{1\}$.

Let $\eta = \tau(\alpha)/\alpha$. Apply (4.2) and its conjugate by $\tau$, taking into account that we are working in an abelian extension of $E$. We obtain

$$\theta = \frac{\tau(\beta)}{\beta} = \frac{\tau\tilde{\sigma}_2(\alpha)}{\tau(\alpha^g)\tau\tilde{\sigma}_1(\alpha)} \left( \frac{\tilde{\sigma}_2(\alpha)}{\alpha^g \tilde{\sigma}_1(\alpha)} \right)^{-1} = \frac{\tilde{\sigma}_2(\eta)}{\eta^g \tilde{\sigma}_1(\eta)} \; .$$

Hence $gh(\eta) \leq 2h(\eta)$ which implies $h(\eta) = 0$ by (4.1). Thus $\eta \in \boldsymbol{\mu}$. Write $\eta$ as $\eta = \eta_1 \eta_2$ with $\eta_1 \in \boldsymbol{\mu}_{p^\infty}$ and with $\eta_2$ of order not divisible by $p$. By Bezout's identity, $\eta_1 \in \mathbb{Q}(\eta) \subseteq L$. Thus there exists an integer $a$ such that $\eta_1 = \zeta_k^a$. By the choice of $\tilde{\sigma}_i$ we see that

$$\frac{\tilde{\sigma}_2(\eta_1)}{\eta_1^g \tilde{\sigma}_1(\eta_1)} = 1 \; .$$

Thus

$$\theta = \frac{\tilde{\sigma}_2(\eta_2)}{\eta_2^g \tilde{\sigma}_1(\eta_2)}$$

has order not divisible by $p$. But $\theta \in \boldsymbol{\mu}_{p^\infty}$ and $\theta \neq 1$. Contradiction.

Applying (3.1) with $\alpha \leftarrow \beta$ we get $h(\beta) \geq c$. By (4.1) and (4.2),

$$h(\beta) \leq (g+2)h(\alpha) \leq (6d_0d+7)h(\alpha)\ .$$

Thus

$$h(\alpha) \geq c'$$

with $c' = c/(6d_0d+7)$.

□

We are now in position to prove Theorem 1.2. Let $K$ be a number field and let $L/K$ be an infinite Galois extension with Galois group $G$. Let $E \subseteq L$ be the subfield fixed by $Z(G)$ and assume that $E/K$ has local degree at some prime $\wp$ bounded by $d_0$. Let $\alpha \in L^*$ not a root of unity. We choose a subfield $L'$ containing $\alpha$ and such that $L'/K$ is Galois. We put $E' = L' \cap E$. Then it is easy to see that $L'/E'$ is Galois and $\mathrm{Gal}(L'/E')$ is contained in the center of $\mathrm{Gal}(L'/K)$. Moreover $E'/K$ has local degree at $\wp$ bounded by $d_0$. By Proposition 4.2, the height of $\alpha$ is bounded from below by a positive constant depending only on $\wp$, $d_0$ and on $[K:\mathbb{Q}]$. Theorem 1.2 follows.

# 5 Property (B) and field extensions

In this section we show that the Property (B) is not generally preserved by taking a finite extension. As remarked in the introduction, this on the contrary holds for the Property (N).

Let $\mathbb{Q}^{tr}$ be the compositum of all totally real extensions. Thus $\mathbb{Q}^{tr}$ is a Galois extension of $\mathbb{Q}$ and $\alpha \in \mathbb{Q}^{tr}$ if and only if $\alpha$ is totally real. We denote by $i$ a square root of $-1$ in $\overline{\mathbb{Q}}$. Note that $\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}$ is also Galois, as the composite of the Galois extensions $\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q}$ and $\mathbb{Q}(i)/\mathbb{Q}$. Let $\tau$ be the generator of $\mathrm{Gal}(\mathbb{Q}^{tr}(i)/\mathbb{Q}^{tr})$. Then for any $\mathbb{Q}$-embedding $\sigma\colon \mathbb{Q}^{\mathrm{tr}}(i) \hookrightarrow \mathbb{C}$ we have $\overline{\sigma} = \sigma\tau$. This implies that if an archimedean absolute value of $\alpha \in \mathbb{Q}^{tr}(i)$ is 1 then all its archimedean absolute values are equal to 1. The following lemma shows that the converse is also true.

**Lemma 5.1** *Let $\alpha \in \overline{\mathbb{Q}}$ be such that all its archimedean absolute values are equal to* 1. *Then $\alpha \in \mathbb{Q}^{tr}(i)$.*

**Proof.** We define

$$a = \frac{1}{2}(\alpha + \alpha^{-1}), \quad b = \frac{1}{2i}(\alpha - \alpha^{-1})\ .$$

Then $\alpha = a + bi$ and $a, b \in \mathbb{Q}^{tr}$. Indeed, let $\sigma\colon \mathbb{Q}^{\mathrm{tr}}(i) \hookrightarrow \mathbb{C}$. Since

$$1 = |\sigma\alpha|^2 = \sigma\alpha \cdot \overline{\sigma\alpha}\ ,$$

we have

$$\sigma a = \frac{1}{2}(\sigma\alpha + \overline{\sigma\alpha}) = \mathrm{Re}(\sigma(\alpha)), \quad \sigma b = \frac{1}{2\sigma(i)}(\sigma\alpha - \overline{\sigma\alpha}) = \mathrm{Im}(\sigma(\alpha))\ .$$

□

**Remark 5.2** We recall that a number field $L$ is a CM field if it is a totally complex quadratic extension of a totally real number field. It is well-known (see for instance [Wa], p.38) that in a CM field $L$ the complex conjugation of $\mathbb{C}$ defines an involution $\tau$ of $L$ which is independent of the embedding into $\mathbb{C}$., *i.e.* for any $\mathbb{Q}$-embedding $\sigma\colon L \hookrightarrow \mathbb{C}$ we have $\overline{\sigma} = \sigma\tau$. Let $\alpha \in L$. The argument of the proof of Lemma 5.1 shows that

$$a = \frac{1}{2}(\alpha + \tau(\alpha)), \quad b = \frac{1}{2i}(\alpha - \tau(\alpha)) \ .$$

are totally reals. Thus $\alpha = a + ib \in \mathbb{Q}^{\mathrm{tr}}(i)$. This proves that any CM field is contained in $\mathbb{Q}^{\mathrm{tr}}(i)$ (and actually $\mathbb{Q}^{\mathrm{tr}}(i)$ is the compositum of all CM fields).

We are now in position to give the promised example.

**Example 5.3** *The field $\mathbb{Q}^{tr}$ satisfies (B), but its quadratic extension $\mathbb{Q}^{tr}(i)$ does not.*

**Proof.** For the first assertion, see [Sc] and [Sm]. For the second one, [Am-Nu], Theorem 1.3, shows that there exists an infinite sequence $(\alpha_k)$ of algebraic numbers such that the fields $\mathbb{Q}(\alpha_k)$ are CM-fields, $\alpha_k$ is not a root of unity, and $h(\alpha_k) \to 0$. By remark 5.2, $\mathbb{Q}(\alpha_k) \subseteq \mathbb{Q}^{tr}(i)$. Thus the field $\mathbb{Q}^{tr}(i)$ does not satisfy (B). A more direct example is the following. For $k \in \mathbb{N}$ let

$$\alpha_k = \left(\frac{2-i}{2+i}\right)^{1/k} \ .$$

Then all the archimedean absolute values of $\alpha_k$ are equal to 1. Thus, by Lemma 5.1, $\alpha_k \in \mathbb{Q}^{tr}(i)$. Obviously $\alpha_k$ is not a root of unity and $h(\alpha_k) \to 0$ (note, however, that extracting roots is not the only manner to construct number of small height in $\mathbb{Q}^{tr}(i)$. See again [Am-Nu], sections 4 and 5 for details).

□

In view of this example, it may not be out of place to study the Galois group of $\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q}$. The *absolute* Galois group of $\mathbb{Q}^{\mathrm{tr}}$ is known. By a result of Freid, Haran and Völklein (see [Fr-Ha-Vo]) $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{tr}})$ is freely generated by a subset of involutions, homeomorphic to the Cantor set. Nevertheless, nothing is apparently known on $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$.

By a well known theorem of Artin-Schreier-Baer (see [Ar-Sc] and [Ba]) the only non trivial elements of finite order in the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ are the complex conjugations. In the present situation we have:

**Theorem 5.4** *There is no automorphism of finite order $> 1$ in* $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$.

We shall give a proof of this theorem in section 7. For the moment, let us pause for some consequences of this statement.

Let $G$ be a profinite group such that *any* Galois extension $L/\mathbb{Q}$ with Galois group $G$ satisfy (B). Let $L/\mathbb{Q}$ be any of such extensions. We could ask if any finite extension of $L$ satisfy again (B).

The group $G = \mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$ provide a counterexample to this assertion. Indeed, if $L/\mathbb{Q}$ has Galois group $G$, then $L \subseteq \mathbb{Q}^{\mathrm{tr}}$. Otherwise we could find an involution in $G$, contradicting Theorem 5.4. By the quoted result of [Sc] and [Sm], any Galois extension $L/\mathbb{Q}$ with Galois group $G$ satisfy (B).

Thus $G$ is a profinite group such that any Galois extension $L/\mathbb{Q}$ with Galois group $G$ satisfy (B). However, as proved in example 5.3, $\mathbb{Q}^{\mathrm{tr}}(i)$ is a quadratic extension of $L = \mathbb{Q}^{\mathrm{tr}}$ which does not satisfy (B) and $\mathrm{Gal}(L/\mathbb{Q}) = G$.

The situation seems to be different if we allow base change.

**Definition 5.5** *Let $G$ be a profinite group. We say that $G$ has the Property (B) if for any number field $K$ and for any Galois extension $L/K$ with Galois group $G$, the field $L$ satisfies (B).*

By Galois theory, a profinite group $G$ satisfies (B) if and only *at least one of its subgroups of finite index* satisfies (B). Indeed, let $H$ be a subgroup of finite index of $G$ which satisfies (B). Let $L/K$ be a Galois extension of a number field $K$ such that $\mathrm{Gal}(L/K) = G$. Then $L^H$ is a finite extension of $K$, hence a number field. Since $\mathrm{Gal}(L/L^H) = H$ satisfies (B), the field $L$ satisfies (B).

We remark that $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$ *does not* satisfy (B). Indeed, $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}(i) \cong \mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$ and the field $\mathbb{Q}^{\mathrm{tr}}(i)$ does not satisfy (B).

We also remark that abelian groups and groups with finite exponent satisfy (B). Moreover, let $L/K$ be a Galois extension of a number field with Galois group abelian or of finite exponent. Then any finite extension of $L$ satisfies again (B), as we have already seen in the introduction in the special case $K = \mathbb{Q}$.

More generally, let $G$ be a profinite group such that *all its subgroups of finite index* satisfy (B) (this is the case for abelian groups and for groups of finite exponent). Then any finite extension $E$ of a Galois extension $L/K$ of a number field satisfies (B), provided that $\mathrm{Gal}(L/K) = G$. To see this, select a primitive element $\alpha \in E$ over $L$. Thus $E = L(\alpha)$ and, by Galois theory $L(\alpha)/K(\alpha)$ is a Galois extension with Galois group isomorphic to $H = \mathrm{Gal}(L/L \cap K(\alpha)) \subseteq G$ of index $[L \cap K(\alpha) : K] \leq [K(\alpha) : K] < \infty$. Since $K(\alpha)$ is a number field, if $H$ satisfies (B) then $L(\alpha)$ satisfies (B).

These remarks suggest the following questions:

**Problem 5.6** *Let $G$ be a profinite group which satisfy (B).*

*i) Is it true that any subgroup of $G$ of finite index satisfies (B)?*

*ii) Let $K$ be a number field and let $L/K$ be a Galois extension with Galois group $G$. Is it true that any finite extension of $L$ satisfies (B)?*

By the remarks above, i) implies ii).

Let $1 \to H \to G' \to G \to 1$ be a group extension of profinite groups. A positive answer to problem 5.6 ii) would imply that if $H$ is finite and $G$ satisfies (B), then $G'$ satisfies (B). We remark that we cannot replace "$H$ finite" by "$H$ satisfies (B)" in this last statement. Indeed, for $p$ prime the field

$$L = \mathbb{Q}(\mu_{p^\infty}, 2^{1/p}, 2^{1/p^2}, \ldots)$$

obviously does not satisfy (B). However, its Galois group $G'$ over $\mathbb{Q}$ is an extension of a profinite abelian group by an other profinite abelian group:

$$H = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^*, \qquad \text{and} \qquad G = \mathrm{Gal}(L/\mathbb{Q}(\mu_{p^\infty})) \cong \mathbb{Z}_p \ .$$

# 6 Relations with field arithmetic

In this section we explore some speculative relations between Property (B) and field arithmetic.

We recall that a field $K$ is Pseudo Algebraically Closed (PAC) if each absolutely irreducible variety defined over $K$ has a $K$-rational point (see [Fr-Ja], chapter 11, for more details). Obviously an algebraically closed field is PAC. We give some evidences for a negative answer to the following problem:

**Problem 6.1** *Does there exist a PAC field $K \subseteq \overline{\mathbb{Q}}$ which satisfies (B)?*

First we remark that algebraic extensions of PAC fields are again PAC fields by a theorem of Ax-Roquette ([Fr-Ja], corollary 11.2.5). Similarly, if $K$ does not satisfy (B) and if $E/K$ is an algebraic extension, than $E$ does not satisfy (B).

Only few examples of non-trivial PAC subfields of $\overline{\mathbb{Q}}$ are known. For instance, as a consequence of a deep result of Pop, $\mathbb{Q}^{\mathrm{tr}}(i)$ is a PAC field (see [Pop], Theorem $\mathfrak{S}$, p.21 and [Ja-Ra], section 7 before Lemma 7.1). It is an open problem if the maximal solvable extension $\mathbb{Q}^{\mathrm{solve}}$ of $\mathbb{Q}$ is pseudo algebraically closed (see [Fr-Ja], problem 11.5.9 (a)). Observe that both $\mathbb{Q}^{\mathrm{tr}}(i)$ and $\mathbb{Q}^{\mathrm{solve}}$ do not have Property (B) (this is obvious for the second field and it is true for the first one by example 5.3).

An other example of PAC subfield of $\overline{\mathbb{Q}}$ is provided by the compositum $\mathbb{Q}^{\mathrm{symm}}$ of all symmetric extensions of $\mathbb{Q}$ (*i.e.* of all Galois extensions over $\mathbb{Q}$ with Galois group a symmetric group), see [Fr-Ja], Th. 18.10.4. Again, this field does not satisfy (B). To prove this statement, it is enough to find a family $L_1$, $L_2$, ... of symmetric extensions of $\mathbb{Q}$ such that

$$\lim_{n\to+\infty} \inf\{h(\alpha) \mid \alpha \in L_n,\ \alpha \text{ not a root of unity}\} = 0\ . \tag{6.1}$$

We can choose for $\{L_n\}$ the set of splitting fields of $x^p+x+1$ for $p > 3$ prime, $p \not\equiv 1 \bmod 4$. Indeed for $p$ prime $x^p+x+1$ is irreducible and, if $p$ satisfies the said condition, its splitting field is a symmetric extension (see [Ko]). Moreover, let $\alpha$ be a root of $x^p + x + 1$. Then $\alpha$ is not a root of unity and $ph(\alpha) = h(\alpha + 1) \leq h(\alpha) + \log 2$ by well known properties of Weil's height. Thus $h(\alpha) \leq (\log 2)/(p-1)$.

The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is a compact group, thus admits a translation invariant Haar mesure. Let $e \in \mathbb{N}$. By a theorem of Jarden (*PAC Nullstellensatz*, see [Fr-Ja], Th. 18.6.1), for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^e$ the field $\overline{\mathbb{Q}}^{\boldsymbol{\sigma}}$ fixed by $\sigma_1, \ldots, \sigma_e$ is PAC. It is again quite simple to prove that for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^e$ the field $\overline{\mathbb{Q}}^{\boldsymbol{\sigma}}$ does not satisfy (B). For this purpose we quote the following immediate consequence of [Fr-Ja], Lemma 18.5.3.

**Lemma 6.2** *Let $e \in \mathbb{N}$ and let $L_1$, $L_2$, ... be linearly disjoint number fields. Let us assume that $L_1$, $L_2$, ... satisfy (6.1) and in addition*

$$\sum_{n=1}^{\infty} [L_n : \mathbb{Q}]^{-e} = \infty\ .$$

*Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^e$ the field $\overline{\mathbb{Q}}^{\boldsymbol{\sigma}}$ contains infinitely many $L_n$ and hence it does not satisfy (B).*

**Proof.** We apply the quoted lemma of [Fr-Ja] with $K = \mathbb{Q}$ and $\overline{A}_n = \{\mathrm{Gal}(\overline{\mathbb{Q}}/L_n)\}$. Then, the set of $\boldsymbol{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^e$ such that $\sigma_1, \ldots, \sigma_e \in \mathrm{Gal}(\overline{\mathbb{Q}}/L_n)$ for infinitely many $n$

has Haar measure 1. Thus for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^e$ the field $\overline{\mathbb{Q}}^{\boldsymbol{\sigma}}$ contains infinitely many $L_n$. Since $L_1$, $L_2$, ... satisfy (6.1), $\overline{\mathbb{Q}}^{\boldsymbol{\sigma}}$ does not have (B).

□

It is easy to exhibit $L_1$, $L_2$, ... which satisfy the requirements of the lemma. To simplify, let us assume $e = 1$. Then we can simply choose for $\{L_n\}$ the set of $\mathbb{Q}(2^{1/p})$ for $p$ prime (indeed $\sum 1/p = \infty$).

An other central definition in field arithmetic is the hilbertianity. A field $K$ is Hilbertian if it satisfies Hilbert's Irreduciblity Theorem: for every irreducible $f \in K[x, y]$ which is separable in $x$ there exists $a \in K$ such that $f(x, a)$ is irreducible over $K$ (see [Fr-Ja], chapter 12, for more details). As for PAC fields, we could ask for relations between hilbertianity and (B). But now, we do not have any direct implication. Indeed $\mathbb{Q}^{\mathrm{tr}}$ is not hilbertian (choose $f(x, y) = x^2 - y^2 - 1$) and satisfies (B); on the contrary $\mathbb{Q}^{\mathrm{tr}}(i)$ is hilbertian (by Weissauer's Theorem, [Fr-Ja], capter 13, Theorem 13.9.1) and does not satisfy (B). An other example of field with these properties is $\mathbb{Q}^{\mathrm{symm}}$ which is hilbertian (see [Fr-Ja], Theorem 18.10.4) and does not satisfy (B), as already remarked.

# 7 On the Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q})$

The field $\mathbb{Q}^{\mathrm{tr}}$ has a subset of *totally positive* elements, i.e., those all of whose conjugates are nonnegative. We shall repeatedly use the easy observation that:

*A square root of a totally positive element lies in* $\mathbb{Q}^{\mathrm{tr}}$.

Indeed, if $\alpha$ is totally positive, and $\beta^2 = \alpha$, we have $(\sigma\beta)^2 = \sigma\alpha$, which is real and $\geq 0$ for every $\mathbb{Q}$-embedding $\sigma : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$; hence $\sigma\beta \in \mathbb{R}$ for each such $\sigma$, as asserted.

We shall now prove Theorem 5.4. Let $\sigma$ be a non trivial $\mathbb{Q}$-automorphism of finite order of the field of totally real algebraic numbers. By replacing $\sigma$ with a power of it, we may suppose that its order is a prime $l$. We shall derive a contradiction. Let us start with the

**Case $l = 2$.**

Since $\sigma$ is supposed to have order 2, its fixed field $F$ is such that $[\mathbb{Q}^{\mathrm{tr}} : F] = 2$. We have $\mathbb{Q}^{\mathrm{tr}} = F(\beta)$ for a $\beta$ such that $\alpha := \beta^2 \in F$.

We shall use the following

**Lemma 7.1** *The number $\alpha$ is a sum of two squares of elements of $F$.*

**Proof.** We shall use a result of Hilbert and Landau (see [La], Exercise 1, p. 461, or [Ra], Theorem. 15.11, p. 224): a totally positive $\alpha$ is a sum of squares in $\mathbb{Q}(\alpha)$. In the Appendix below we shall give a self-contained proof of this result.

Note that since $\beta$ is totally real, $\alpha$ is totally positive. By the quoted result, $\alpha$ is then a sum of squares in $\mathbb{Q}(\alpha)$, hence in $F$. Let $\alpha = a_1^2 + \ldots + a_m^2$, $a_1, \ldots, a_m \in F$, be such a representation with minimal $m$. If $m \geq 2$, let $\xi := a_1^2 + \ldots + a_{m-1}^2$. Since the $a_i$ lie in $\mathbb{Q}^{\mathrm{tr}}$, we have that $\xi$ is totally positive. Hence $\sqrt{\xi}$ is totally real, i.e. there exists $\mu \in \mathbb{Q}^{\mathrm{tr}}$

with $\mu^2 = \xi$. We can write $\mu = p + \beta q$ with $p, q \in F$, and then $\xi = p^2 + \alpha q^2 + 2pq\beta$. Since $\xi \in F$ we must have $pq = 0$, but of course we may assume that $p, q$ do not both vanish. If $p = 0$, then $q \neq 0$ and we obtain a representation of $\alpha$ as a sum of $m - 1$ squares, a contradiction. Then $q = 0$. But then $\xi = p^2$ and $\alpha = p^2 + a_m^2$, as required.

□

By the lemma, we may find $x, y \in F^*$ such that $x^2 - \alpha y^2 = -1$. Set $\gamma := x + \beta y$, so $N(\gamma) = -1$, where $N$ is the norm from $\mathbb{Q}^{\mathrm{tr}}$ to $F$.

We have $N(\gamma^2) = 1$. Set $\eta := 1+\gamma^2$, and denote with an accent the said automorphism (i.e. the conjugation of $\mathbb{Q}^{\mathrm{tr}}$ over $F$). We have $\gamma^2(\gamma')^2 = 1$, so $\eta' = 1 + (\gamma')^2 = 1 + \gamma^{-2} = \eta\gamma^{-2}$.

Since $\gamma \in \mathbb{Q}^{\mathrm{tr}}$, the element $\eta$ is totally positive, whence $\eta = \delta^2$ for some $\delta \in (\mathbb{Q}^{\mathrm{tr}})^*$. Hence $\gamma^2(\delta')^2 = \delta^2$, leading to $\gamma = \pm\delta/\delta'$. But then $N(\gamma) = 1$ and we have a contradiction, concluding the proof in the case $l = 2$.

**Case $l > 2$.**

We recall that $\mathbb{Q}^{\mathrm{tr}}(i)/\mathbb{Q}$ is also Galois, as the composite of the Galois extensions $\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q}$ and $\mathbb{Q}(i)/\mathbb{Q}$. Note that $\mathbb{Q}^{\mathrm{tr}}(i)$ contains all roots of unity (as an immediate consequence of lemma 5.1). We also recall that the complex conjugation of $\mathbb{C}$ defines an automorphism $\tau$ of $\mathbb{Q}^{tr}(i)$ which is independent of the embedding into $\mathbb{C}$. By abuse of notation, we shall denote this automorphism by the usual symbol $\overline{\alpha} := \tau(\alpha)$.

Let $L$ denote the fixed field of $\sigma$ in $\mathbb{Q}^{\mathrm{tr}}$; we may extend $\sigma$ to an automorphism, denoted again $\sigma$, of $\mathbb{Q}^{\mathrm{tr}}(i)$, fixing $i$, so $L(i)$ is the fixed field of $\sigma$ in $\mathbb{Q}^{\mathrm{tr}}(i)$ and $[\mathbb{Q}^{\mathrm{tr}}(i) : L(i)] = [\mathbb{Q}^{\mathrm{tr}} : L] = l$. Note that $\mathbb{Q}^{\mathrm{tr}}(i)$ contains the $l$-th roots of unity, whose degree over $L(i)$ divides $l - 1$; but this degree also divides $l$, whence $L(i)$ contains the $l$-th roots of unity. By Kummer's theory we then have $\mathbb{Q}^{\mathrm{tr}}(i) = L(i)(\beta)$ where $\beta^l =: \alpha \in L(i)$, and $\sigma(\beta) = \theta\beta$ for some primitive $l$-th root of unity $\theta$. Since $L \subset \mathbb{Q}^{\mathrm{tr}}$, $L(i)$ is sent into itself by complex conjugation, so also $\overline{\beta}$ generates $\mathbb{Q}^{\mathrm{tr}}(i)$ over $L(i)$ and $\overline{\beta}^l = \overline{\alpha} \in L(i)$. By Kummer's theory again, we have

$$\overline{\beta} = \gamma\beta^r, \qquad \gamma \in L(i)\ , \tag{7.1}$$

for some $r$ coprime to $l$ (only its residue class mod $l$ matters in (7.1)).

Applying to (7.1) complex conjugation we get $\beta = \overline{\gamma}\overline{\beta}^r$, and using (7.1) in this last equation we obtain

$$\beta = \overline{\gamma}\gamma^r\beta^{r^2},$$

whence $\beta^{r^2-1} \in L(i)$. Since $\beta^l \in L(i)$ and $\beta$ is not in $L(i)$ this yields $r^2 \equiv 1 \pmod{l}$, so $r \equiv \pm 1 \pmod{l}$, and then we may suppose $r = \pm 1$ in (7.1), so also $\overline{\gamma}\gamma^r = 1$.

If $r = 1$ we have $\overline{\gamma}\gamma = 1$ whence (by Hilbert 90 for $L(i)/L$) $\gamma = u/\overline{u}$ for some $u \in L(i)$. Then $\overline{u\beta} = u\beta$, so $u\beta$ is totally real, and then $u\beta \in \mathbb{Q}^{\mathrm{tr}}$. But since $\sigma$ fixes $L(i)$ pointwise and stabilizes $\mathbb{Q}^{\mathrm{tr}}$, this contradicts that $\sigma(\beta)/\beta$ is a primitive $l$-th root of unity, so not totally real.

Therefore we have $r = -1$, and $\beta\overline{\beta} = \gamma \in L(i)$ (actually $\gamma \in L$ since this shows it is totally real).

Note now that $\mathbb{Q}^{\mathrm{tr}}(i) = L(i)(\rho\beta^s)$ for every $\rho \in L(i)^*$ and every $s$ coprime to $l$, hence we may replace $\beta$ with such $\rho\beta^s$ to generate $\mathbb{Q}^{\mathrm{tr}}(i)/L(i)$. We choose $s = 2$ and $\rho = (\beta\overline{\beta})^{-1}$, so $\rho\beta^s = \beta/\overline{\beta} =: \xi$, say, and $\mathbb{Q}^{\mathrm{tr}}(i) = L(i)(\xi)$, where $\mu := \xi^l = \beta^{2l}/\gamma^l \in L(i)$.

All conjugates of $\xi$ have absolute value 1, so all the conjugates of $\xi^{\frac{1}{l}}$ have absolute value 1, and therefore, by lemma 5.1 $\xi^{\frac{1}{l}}$ lies in $\mathbb{Q}^{\rm tr}(i)$, for every choice of the $l$-th root. Note that $(\xi^{\frac{1}{l}})^{l^2} = \xi^l = \mu$.

At this point the proof mimics an argument of Artin, proving that $\mathbb{C}$ has no automorphisms of finite odd order (see Lang's quoted book, p. 299, Cor. 9.3). The polynomial $x^{l^2} - \mu = x^{l^2} - \xi^l$ lies in $L(i)[x]$ and has a root (actually all roots) in $\mathbb{Q}^{\rm tr}(i)$. But $[\mathbb{Q}^{\rm tr}(i) : L(i)] = l$, so the polynomial is reducible. By Capelli's Theorem (see Lang's quoted book, Ch. VIII, Theorem 16), we have $\mu = a^l$ for some $a \in L(i)$. This yields $\xi = \zeta a$ for an $l$-th root of unity $\zeta$, and since $\zeta$ lies in $L(i)$ as noted above, we deduce that $\xi \in L(i)$, a contradiction which proves the theorem.

# 8 Appendix

In this Appendix we provide a self-contained proof of the following result, used in the proof of Lemma 7.1:

**Theorem 8.1** *Let $\alpha$ be a totally real algebraic number. Then an element of $\mathbb{Q}(\alpha)$ is a sum of squares in $\mathbb{Q}(\alpha)$ if and only if it is totally positive.*

This theorem is due to Hilbert and Landau, in a more general form when $\alpha$ is not necessarily totally real and it is required that all embeddings in $\mathbb{R}$ of the relevant number are positive. See Lang's or Rajwade's above-quoted references for a proof which depends on Artin-Schreier's theory of real fields. The simple proof below is independent of this theory and would seemingly work with small modifications also for the more general assertion.

To prove Theorem 8.1 note that one half of the conclusion is clear and so it suffices to work on the assumption that $\alpha$ is totally positive, and to prove that $\alpha$ is a sum of squares in $\mathbb{Q}(\alpha)$.

We let $d := [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and we denote by $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ the (positive) distinct conjugates of $\alpha$ over $\mathbb{Q}$.

There are polynomials $f_1, \ldots, f_d \in \mathbb{R}[x]$ of degree at most $d-1$, and such that $f_i(\alpha_j)$ equals 2 if $i = j$ and 0 otherwise. (Just solve a Vandermonde linear system, or else take $f_i(x) = c_i \prod_{r \neq i}(x - \alpha_r)$ with $c_i = 2\prod_{r \neq i}(\alpha_i - \alpha_r)^{-1}$.)

Let us choose $\epsilon > 0$ as a real positive number $< \frac{\min \alpha_i}{2d \max \alpha_i}$.

By approximating the coefficients of $f_i$ with rational numbers, and squaring, we may then find polynomials $g_1, \ldots, g_d \in \mathbb{Q}[x]$ (also of degree $\leq d-1$) such that, for $i = 1, \ldots, d$,

$$g_i^2(\alpha_i) > 1, \qquad g_i^2(\alpha_j) < \epsilon, \quad j \neq i. \tag{8.1}$$

Define vectors $v_1, \ldots, v_d \in \mathbb{R}^d$ by

$$v_i := (g_1^2(\alpha_i), \ldots, g_d^2(\alpha_i)).$$

Note that $v_1, \ldots, v_d$ are linearly independent: if $t_1 v_1 + \ldots + t_d v_d = 0$ with real $t_i$ not all 0, we may assume on dividing by the coefficient of maximal absolute value, that $t_r = 1$ while $|t_i| \leq 1$ for $i = 1, \ldots, d$. The relation implies $t_1 g_r^2(\alpha_1) + \cdots + t_d g_r^2(\alpha_d) = 0$, whence $1 < g_r^2(\alpha_r) \leq (d-1)\epsilon$, a contradiction with the said choice of $\epsilon$.

Then we may find (uniquely !) real numbers $c_1, \ldots, c_d$ such that

$$\alpha_i = c_1 g_1^2(\alpha_i) + \cdots + c_d g_d^2(\alpha_i), \qquad i = 1, \ldots, d. \tag{8.2}$$

The $c_i$ are surely in $\mathbb{Q}(\alpha_1, \ldots, \alpha_d)$, but must actually be in $\mathbb{Q}$, as can be seen by uniqueness and taking conjugates of these relations, or also directly by noting that the independence of the $v_i$ amounts to the fact that $g_1^2(\alpha), \ldots, g_d^2(\alpha)$ is a basis of $\mathbb{Q}(\alpha)/\mathbb{Q}$.

We contend that $c_i \geq 0$ for all $i$. Indeed, let $M := \max |c_i|$ and suppose that $M = |c_r|$. Evaluating (8.2) at $i = r$ and recalling (8.1) we have

$$M \leq \epsilon(d-1)M + |\alpha_r| \leq M/2 + \max |\alpha_i|,$$

proving that $M \leq 2 \max |\alpha_i|$. Now, suppose by contradiction that $c_s < 0$, and evaluate (8.1) at $i = s$. We obtain

$$0 < \alpha_s \leq \sum_{j \neq s} c_j g_j^2(\alpha_s) \leq M(d-1)\epsilon \leq 2(d-1)(\max |\alpha_i|)\epsilon \; .$$

But this contradicts our choice of $\epsilon$.

Then the $c_i$ are nonnegative rationals, and therefore each of them is a sum of squares of rational numbers: for $a, b$ positive integers, the fraction $\frac{a}{b}$ is the sum of $ab$ equal squares $\frac{1}{b^2}$. Then, relation (8.2) for $i = 1$ proves the sought conclusion.

□

**Remark 8.2** Note that the proof shows that only $d$ distinct squares (each repeated a suitable number of times) suffice to represent $\alpha$ in the sought shape.

# References


[Am-Dv] F. Amoroso and R. Dvornicich – "A Lower Bound for the Height in Abelian Extensions." *J. Number Theory* **80** (2000), no 2, 260–272.

[Am-Nu] F. Amoroso and F. Nuccio, "Algebraic Numbers of Small Weil's height in CM-fields: on a Theorem of Schinzel." *J. Number Theory* **122** (2007), no 1, 247–260.

[Am-Za] F. Amoroso and U. Zannier, "A relative Dobrowolski's lower bound over abelian extensions." *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **29** (2000), no. 3, 711–727.

[Am-Za2] F. Amoroso and U. Zannier, "A uniform relative Dobrowolski's lower bound over abelian extensions." *Bull. London Math. Soc.*, **42** (2010), no. 3, 489–498.

[Ar-Sc] E. Artin and O. Schreier, "Algebraische Konstruktion reeller Körper", pp. 258–272 in: Artins Collected Papers (Ed. S. Lang and J. Tate), Springer-Verlag, New York, 1965.

[Ba] R. Baer, "Die Automorphismengruppe eines algebraisch abgeschlossen Körpers der Charakteristik 0", *Math. Zeit.* **117**, (1970), 7–17.

[Bo-Za] E. Bombieri and U. Zannier, "A note on heights in certain infinite extensions of $\mathbb{Q}$." *Rend. Mat. Acc. Lincei (9)*, **12** (2001), 5–14.

[Ch] S. Checcoli, "On fields of algebraic numbers with bounded local degrees." PhD Thesis. University of Pisa. 2010.

[Dv-Za] R. Dvornicich and U. Zannier, "On the properties of Northcott and of Narkiewicz for fields of algebraic numbers." *Funct. Approx. Comment. Math.* **39** (2008), part 1, 163–173.

[Fr-Ha-Vo] M. D. Fried, D. Haran and H. Völklein, "Absolute Galois group of the totally real numbers". *C. R. Acad. Sci. Paris Sér. I Math.* **317** (1993), no. 11, 995–999.

[Fr-Ja] M. D. Fried and M. Jarden, *Field arithmetic*. Third edition. Ergebnisse der Math. und ihrer Grenz. 11. Springer-Verlag, Berlin, 2008.

[Ja-Ra] M. Jarden and A. Razon, "Pseudo algebraically closed fields over rings", Isr. J. Math. **86** (1994), 25–59.

[Ko] K. Komatsu "On the Galois group of $x^p + ax + a = 0$". *Tokyo J. Math.* **14** (1991), no. 1, 227–229.

[La] S. Lang, *Algebra*. Revised third edition. Graduate Texts in Mathematics, **211**. Springer-Verlag, New York, 2002.

[Hab] P. Habegger, "Small Height and Infinite Non-Abelian Extensions". Preprint 2011. arXiv:1109.5859v1

[Pop] F. Pop, "Over Large Fields". *Annals of Math.*, **144** (1996), no. 1, 1–34.

[Ra] A. Rajwadei, *Squares*. London Mathematical Society Lecture Note Series, **171**. Cambridge University Press, Cambridge, 1993.

[Sc] A. Schinzel, "On the product of the conjugates outside the unit circle of an algebraic number." *Acta Arith.*, **24** (1973), 385–399. Addendum, *ibidem*, **26** (1973), 329–361.

[Sm] C. J. Smyth, "On the measure of totally real algebraic numbers. I" *J. Austral. Math. Soc., Ser. A*, **30** (1980-1), 137–149. "On the measure of totally real algebraic numbers. II" *Math. Comp.*, **37** (1981), 205–208.

[Wa] L. C. Washington, "Introduction to Cyclotomic Fields". Springer-Verlag, New York, 1982.